SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA USING ANONYMOUS KEYS

BACKGROUND OF THE INVENTION

1. Field of the invention

The present invention relates generally to computer security and more specifically to allow the secure transfer and receipt of data between computers using anonymous keys.

2. Description of the Prior Art

In order to securely transfer data between computers on the Internet, various different types of encryption/decryption methods are used. One way of securely transferring data over the Internet includes the use of a public key/private key system.

A public key is provided by some designated authority as a key that, combined with a private key derived from the public key, can be used to effectively encrypt and decrypt messages and digital signatures.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as

RSA) by a certificate authority. The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key counterpart by someone else who has the public key.

Public key cryptography generally requires a large mathematical decomposition in order to work effectively. Generally, the length of a private key is in the order of 64 bytes. Decomposing these relatively small private keys requires considerable computational power. Public key cryptography is typically used as a one-way encryption and if a private key is changed, then everyone else that has the public key counterpart must receive a new public key.

Thus, it would be desirable to provide a system and method of securing data that is easy to use, allows a user to have only a private key unknown to anyone else, does not require a public key, allows for a larger size private key for high security, uses less computation power than public key cryptography, and can be used in two directions.

SUMMARY OF THE INVENTION

A system and method is provided of securely transmitting data between two computers over a network, such as the Internet, using anonymous keys that are private only to each user and are not shared with anyone else. The data is first encrypted at a first computer with a first private key into a first encrypted data file. The first encrypted data file is then transmitted to a second computer, wherein the first encrypted data file is encrypted with a second private key into a second encrypted data file. The second encrypted data file is then sent to the first computer, wherein the second encrypted data file is now decrypted with the first private key, known to the user at the first computer, into a third encrypted data file. The third encrypted data file is then sent to the second computer, wherein the third encrypted data file can not be fully decrypted into the original data file using the second private key.

Associative properties of encryption and decryption are used and allow for the use of large private keys in order to obtain a high-level of security. Additionally, the computational power to encrypt and decrypt data is significantly lower than the public key system since the encryption method is based on one private key and not on a public key and private key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention may be better understood, and its numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying illustrations. For simplicity and ease of understanding, common numbering of elements is employed where an element is the same in different illustrations.

FIG. 1 is a schematic diagram illustrating a client transmitting secure data to a server over the Internet, in accordance with the present invention;

FIG. 2 is a block diagram of the server computer shown in FIG. 1, in accordance with the present invention;

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module located within the server computer of FIG. 2; and

FIG. 4 is a block diagram of the client computers shown in FIG. 1, in accordance with the present invention;

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module located within the client computers of FIG. 4; and

FIG. 6 is a flowchart of a method illustrating how a client, having a private key, passes encrypted data to a server computer, according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following is a detailed description of illustrative embodiments of the present invention. As these embodiments of the present invention are described with reference to the aforementioned illustrations, various modifications or adaptations of the methods and or specific structures described may become apparent to those skilled in the art. All such modifications, adaptations, or variations that rely upon the teachings of the present invention, and through which these teachings have advanced the art, are considered to be within the spirit and scope of the present invention. Hence, these descriptions and drawings should not be considered in a limiting sense, as it is understood that the present invention is in no way limited to only the embodiments illustrated.

Referring now to FIG. 1, a schematic diagram illustrates a server 100 used to receive encrypted data from a client computer 102 through the Internet 106 using anonymous keys that are private and unknown to others.

FIG. 2 is a block diagram of the server computer 100 shown in FIG. 1. Server 100 includes a CPU 202, a RAM 204, a non-volatile memory 206, an input device 208, a display 210, and an Internet interface 212 for providing access to the Internet.

FIG. 3 is a block diagram of one embodiment of the non-volatile memory module 206 located within the server computer 100 of FIG. 2. The non-volatile memory 206 includes an encrypt/decrypt engine 302, and a secure data database 304 for storing secured data.

The encrypt/decrypt engine 302 is programmed to encrypt and decrypt data using a password or a key provided by the user. The encryption/decryption engine is programmed to use associative properties that would provide an associative-type of algorithm for the encryption and decryption of data. For example, if the data is encrypted by 'X' then that would result in encrypted data(X). If encrypted data(X) is then encrypted by 'Y' then that would result in encrypted data(X*Y). If encrypted data(X*Y) is decrypted by 'X' then that would result in encrypted data(Y). If encrypted data(Y) is decrypted by 'Y' then that would result in obtaining the original un-encrypted data. The computation power required to encrypt and decrypt data using this system and method is much less than the computational power required in a public/private key system, therefore longer keys can be used to provide an extremely high-level of security.

FIG. 4 is a block diagram of a client computer 102 shown in FIG. 1. Client 102 includes a CPU 402, a RAM 404, a non-volatile memory 406, an input device 408, a display 410, and an Internet interface 412 for providing access to the Internet.

FIG. 5 is a block diagram of one embodiment of the non-volatile memory module 404 located within the client 102 of FIG. 4. The non-volatile memory 406 includes an encrypt/decrypt engine 502 for encrypting and decrypting data. The encrypt/decrypt engine 502 can also be stored in RAM 404, and excellent results can be obtained when the encrypt/decrypt engine is served up as a Java™ applet to the client 102, thereby eliminating the need for the client to install his own encrypt/decrypt engine on his hard drive.

FIG. 6 is a flowchart of a method illustrating how a client, with a private key, passes data securely encrypted to a server computer through the Internet in accordance with the invention. It is not necessary for the data to pass to a server computer, it can equally work between two client computers. The process begins at step 600. A user enters data on the client computer at step 602. At step 604 the data is encrypted with the encrypt/decrypt engine using the user's private key (E1) and the once-encrypted data (D1) is sent over the Internet to the server.

At step 606 the server encrypts the once-encrypted data with the server private key (E2) and the twice-encrypted data [(D1)*(D2)] is sent back to the client over the Internet. At step 608 the client re-enters his private key and decrypts the twice-encrypted data with his private key resulting in once-encrypted data (D2) that is encrypted with the server private key. The once-encrypted data (D2) is sent over the Internet back

to the server. At step 610 the server can decrypt the once-encrypted data with the server private key (E2) to obtain full access to the original data fully decrypted. The server can then store the data in a secure data database 304 or process the data accordingly. The process then ends at step 612.

Various different modifications can be made to this invention, however, it is essential that the original data is encrypted at least twice, preferably with different private keys, prior to decrypting the data. Furthermore, the data must be sent back-and-forth between the client and server at least three times. This invention is ideal for transmitting small amounts of data, such as a personal identification number, however, the applications of this invention increase as the speed of transmission between computers increases.

The private key of both the client and server is not known by anybody else, therefore, the private key can be different every time a user utilizes this system and method of transmitting data. The private keys can also be very long (i.e. 1000 bytes) and could include biometric data, such as a digitized fingerprint of the user. Since this secure system and method of transmitting encrypted data utilizes a totally private key unknown to others, the various different applications of this invention are virtually limitless. Furthermore, the encrypted data would be virtually impossible to decrypt by a hacker since private keys can be

much longer than a typical private key (64 bytes) used in a private/public key system.